

Dirección General de Tecnología
Departamento de Gestión Informática

PROCEDIMIENTO INTERACTIVO PARA PROCESOS CRIPTOGRAFICOS

SUCED – Sistema Unificado de Certificación Digital

Septiembre 9 de 2014

Versión 1.0



CONTENIDO



1 INTRODUCCIÓN

1.1 OBJETO

El presente documento tiene como fin establecer el procedimiento para el uso del cliente Suced-GUI, con el cual se realiza las operaciones **interactivas** de procesos criptográficos (Firma digital, cifrado, verificación y descifrado) de archivos por las entidades financieras, tales archivos son trasmitidos al Banco de la República a través de los canales dedicados y/o Internet. La definición del canal de comunicación a ser usado dependerá de la definición propia del sistema de información con el que se esté realizando la integración.

1.2 ALCANCE DEL DOCUMENTO

Este documento define el procedimiento, políticas, costos y demás reglas para el uso del servicio interactivo para realizar procesos criptográficos de archivos.

1.3 AUDIENCIA

Este documento está dirigido a las entidades financieras que desean utilizar un modelo interactivo para los procesos criptográficos de archivos.



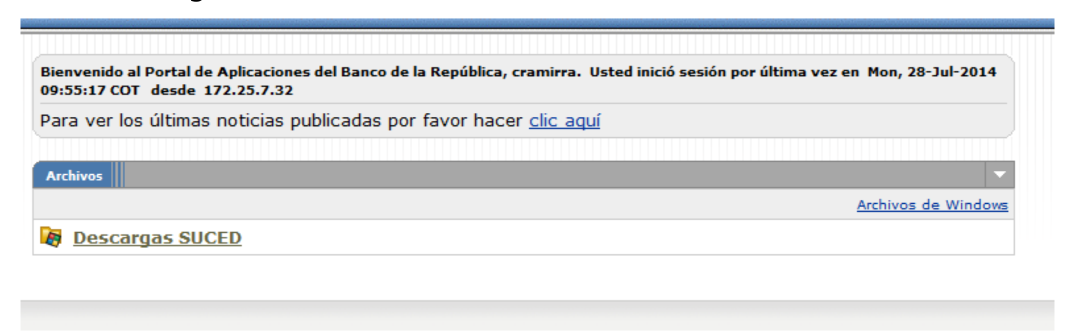
2 PRERREQUISITOS

Para la implementación de procesos criptográficos en modo interactivo siendo usuario de wsebra, se deben tener en cuenta los siguientes prerrequisitos:

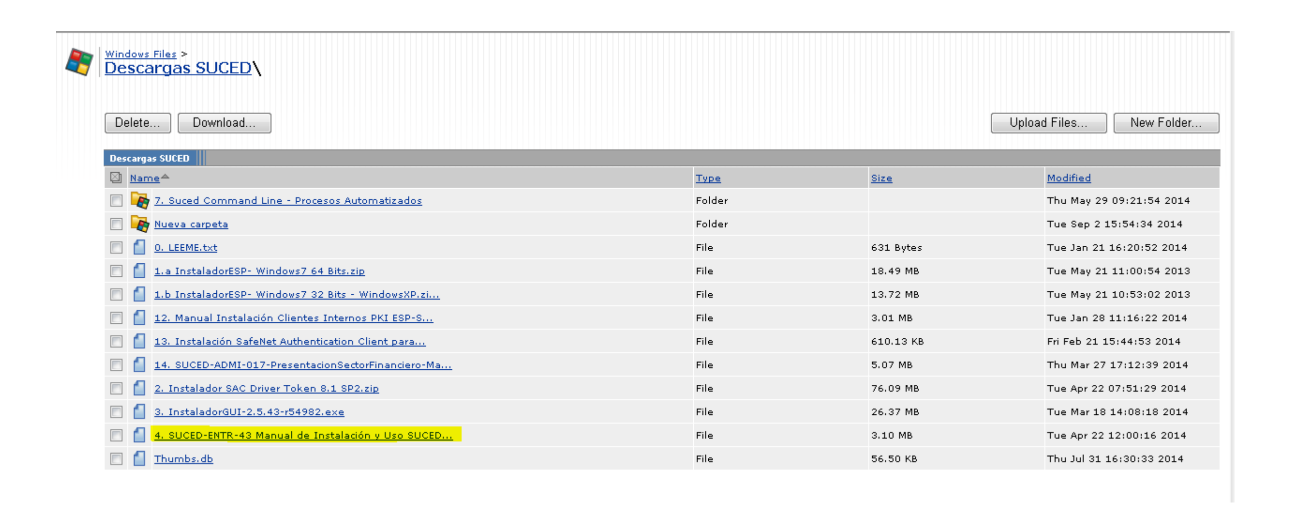
2.1 DESCARGA SUCED-GUI

La descarga del ***SUCED_GUI*** se debe realizar a través del portal https://caribe.banrep.gov.co/emisor

Ingresar en ***Descargas SUCED***



Descargar el manual de instalación "4. SUCED-ENTR-43 Manual de Instalación y Uso SUCEDGUI.pdf"





Una vez descargado el Manual, se deben seguir las instrucciones de instalación descritas en la sección 3 (Instalacion) del manual "***4. SUCED-ENTR-43 Manual de Instalación y Uso SUCEDGUI.pdf***".

Para realizar las operaciones criptográficas de firma, cifrado, descifrado y verificación se requiere del uso de un certificado digital. Ver sección 3 de este documento.

2.2 ACCESOS REQUERIDOS

Para la correcta operación del cliente Interactivo SUCED-GUI para los procesos criptográficos de archivos, se hace necesario que las máquinas de la entidad financiera tengan los siguientes accesos:

Canal	IP	Nombre	servicio	Descripción
SEBRA Dedicado	192.168.61.17	nukak.banrep.gov.co (Pruebas)	TCP/443	Acceso a Bus de Servicios (OSB) del ambiente de pruebas
	192.168.X.X	awa.banrep.gov.co (Producción)	TCP/443	Acceso a Bus de Servicios (OSB) del ambiente de Producción
Internet	X.X.X.X	cuza.banrep.gov.co	TCP/443	Acceso a Bus de Servicios (OSB) del ambiente de pruebas
	X.X.X.X	Nemcatacoa.banrep.gov.co	TCP/443	Acceso a Bus de Servicios (OSB) del ambiente de Producción.

IMPORTANTE: Cada entidad financiera será responsable de configurar el enrutamiento y permisos de conexión a las direcciones anteriormente referenciadas, tanto en las redes internas de la entidad, como de solicitarlo y probarlo con el respectivo proveedor del canal dedicado.

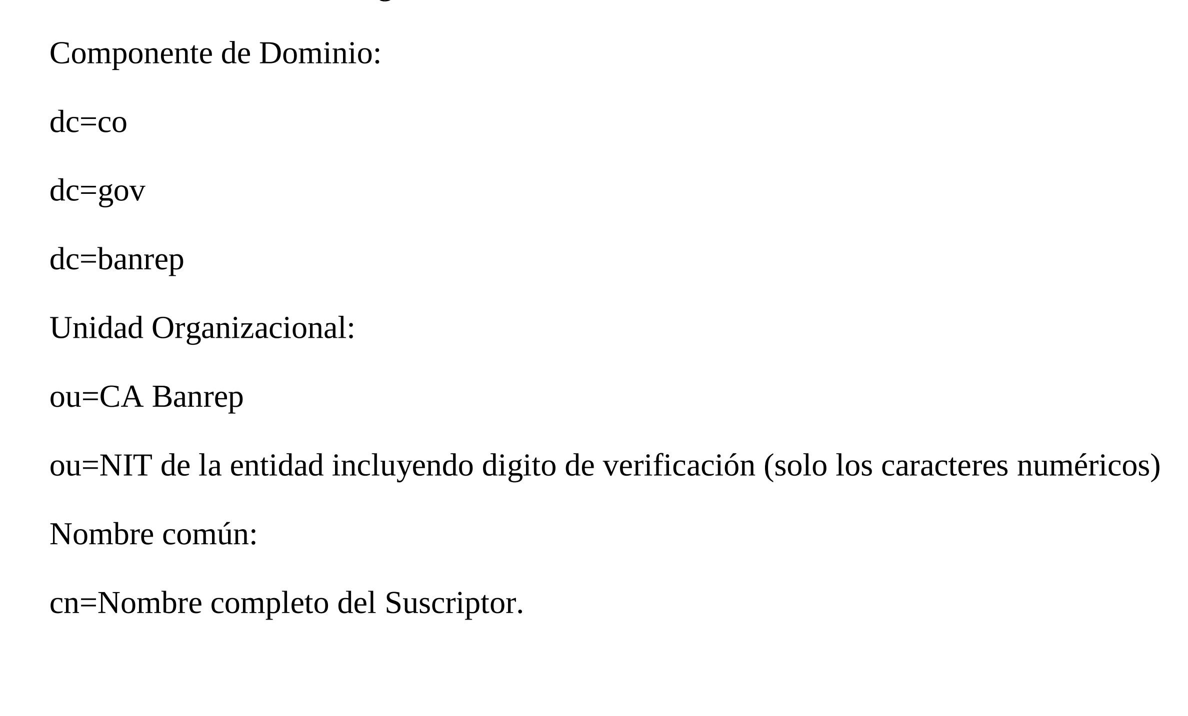
3 SOLICITUD DE CERTIFICADO

Un certificado para realizar procesos ***interactivos***, hace referencia a un certificado emitido a nombre de una persona y debe ser de uso exclusivo por él (este role se denomina

Suscriptor). El certificado deberá ser solicitado por el Delegado con Responsabilidad Administrativa según lo mencionado en el formulario BR-3-598-0.xls, el cual está publicado en el sitio web del Banco (http://www.banrep.gov.co/es/pki-formatos-administrativos.)

El uso correcto del certificado estará a cargo y bajo responsabilidad del Suscriptor y del Delegado con Responsabilidad Administrativa de la Entidad. (Ver Documento "Declaración de Prácticas de Certificación para la ***CA Banrep",*** ubicado en http://www.banrep.gov.co/es/contenidos/page/declaraci-n-pr-cticas-certificaci-n-ca-banrep).

El Certificado del suscriptor para realizar los procesos criptográficos interactivos estará en formato ***PKCS11*** (Token Criptografico) y tendrá la siguiente nomenclatura en la composición de su CN (Common Name). El DN para los Suscriptores de las Entidades Usuarias está formado de la siguiente manera:



Componente de Dominio:

dc=co

dc=gov

dc=banrep

Unidad Organizacional:

ou=CA Banrep

ou=NIT de la entidad incluyendo digito de verificación (solo los caracteres numéricos)

Nombre común:

cn=Nombre completo del Suscriptor.

Ejemplo:

DN: cn=Pedro Perez, ou=8030130231,ou=CA Banrep, dc=Banrep, dc=gov, dc=co



El Certificado del suscriptor tendrá una vigencia de dos (3) años, el Banco de la República informará vía correo electrónico (Que este registrado en la solicitud BR-3-598-0.xls) los próximos certificados a expirar y a fecha de expiración del certificado, así:

El primer día calendario del mes se informaran los certificados a expirar en los siguientes 60 días.

Todos los días se informaran los certificados a expirar dentro de los siguientes 15 días.

La Entidad Financiera mediante el Delegado con Responsabilidad Administrativa será responsable de solicitar la creación del nuevo certificado. Para revisar los términos y condiciones del servicio de creación de certificados. (Ver Documento de Declaración de Practicas de Certificación para la ***CA Banrep*** en ubicado en http://www.banrep.gov.co/es/contenidos/page/declaraci-n-pr-cticas-certificaci-n-ca-banrep).

4 PROCESOS CRIPTOGRÁFICOS

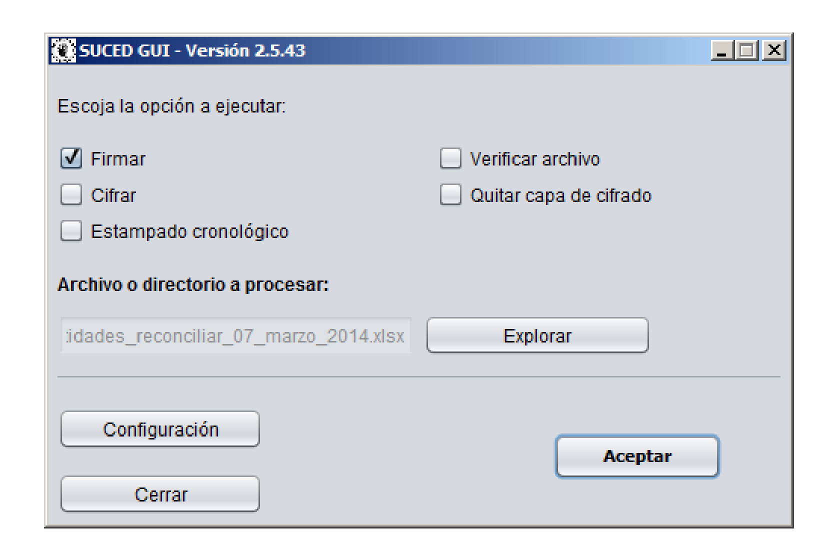
Una vez cumplidos los prerrequisitos mencionados en la sección 2, por favor dirigirse al escritorio y ejecutar SUCED.exe.

*Importante: Si se desea obtener detalles técnicos sobre el funcionamiento de Suced-GUI, por favor observar el manual “4. SUCED-ENTR-43 Manual de Instalación y Uso SUCEDGUI.pdf”, disponible en https://caribe.banrep.gov.co/emisor

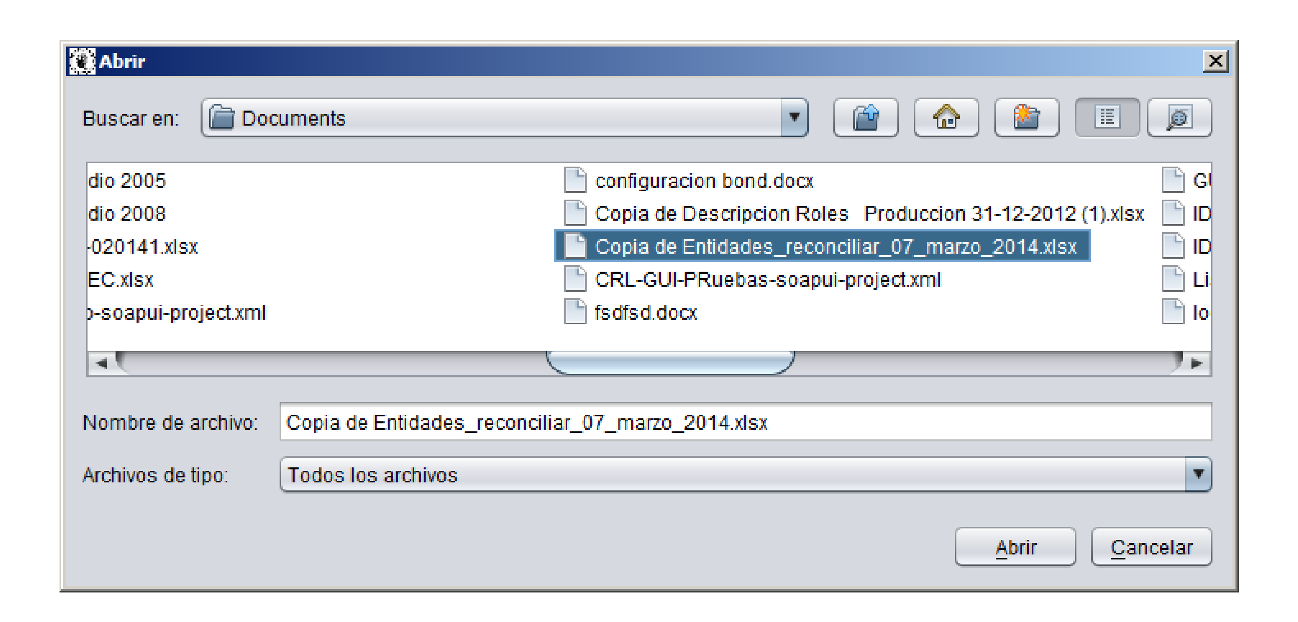
4.1 OPERACIONES DE FIRMA DIGITAL

Para operaciones de Firma Digital, seleccionar firmar,



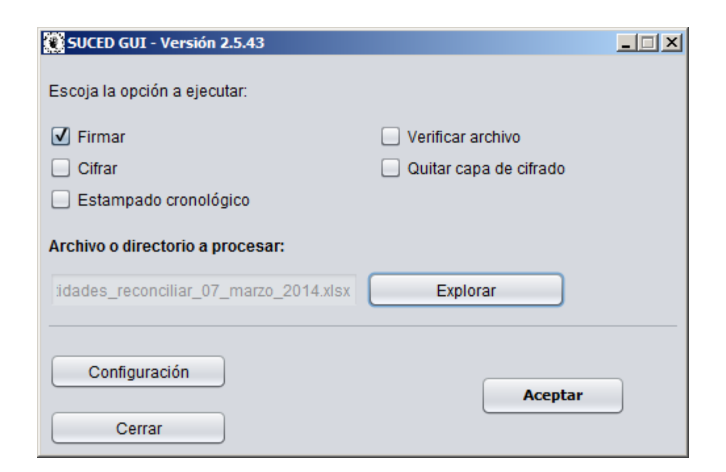


En la opción ***Explorar***, seleccionar el archivo que se desea firmar.

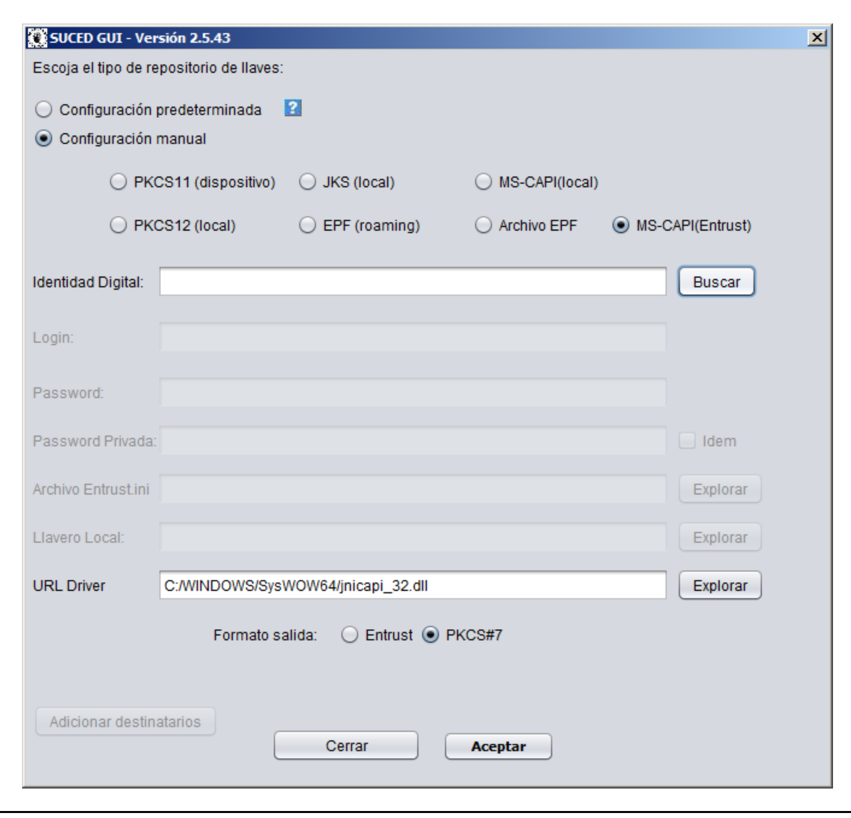


Dar click en ***Aceptar***, el sistema nos mostrará una pantalla como la siguiente:



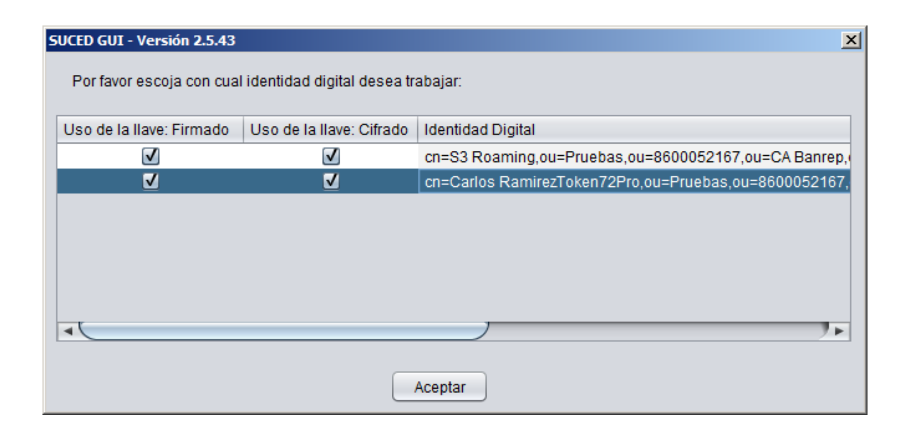


En esta sección, si **NO** se han seguido los pasos mencionados en la sección "4.7 Optimización de pasos SUCED GUI" se debe seleccionar la opción "***Configuración Manual***", y la opción ***MS-CAPI (Entrust)***. De lo contrario usar configuración predeterminada.



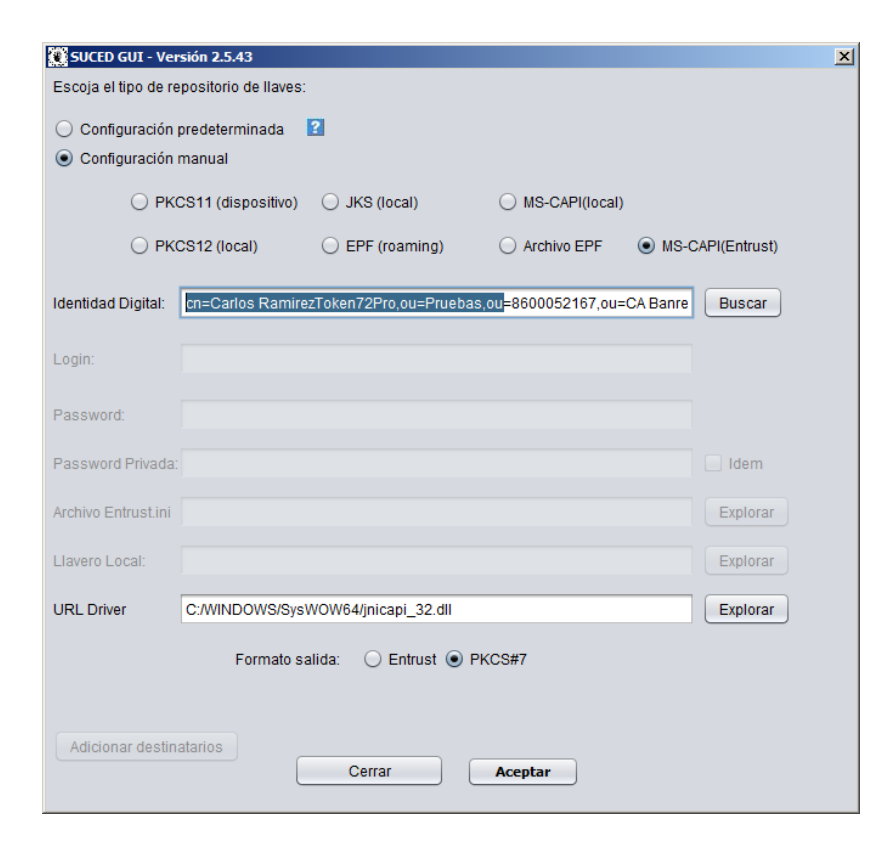


Procedemos a seleccionar la Opción "Buscar", si se tienen varios Tokens conectados y/o credenciales, el sistema permitirá escoger la credencial que se desea usar.



Una vez seleccionada la credencial se procede a dar clic en el botón "***Aceptar***", de forma que el certificado quede elegido:

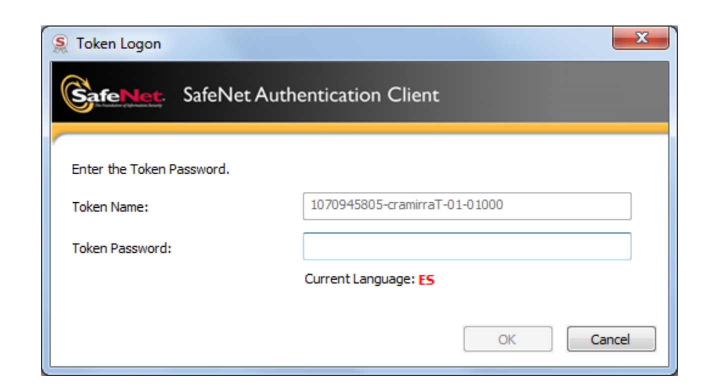




Seleccionar de acuerdo al formato de salida esperada "***Entrust***" para generar formato ***.ent*** o ***PKCS#7*** para generar formato ***.p7z***, según sea el caso.

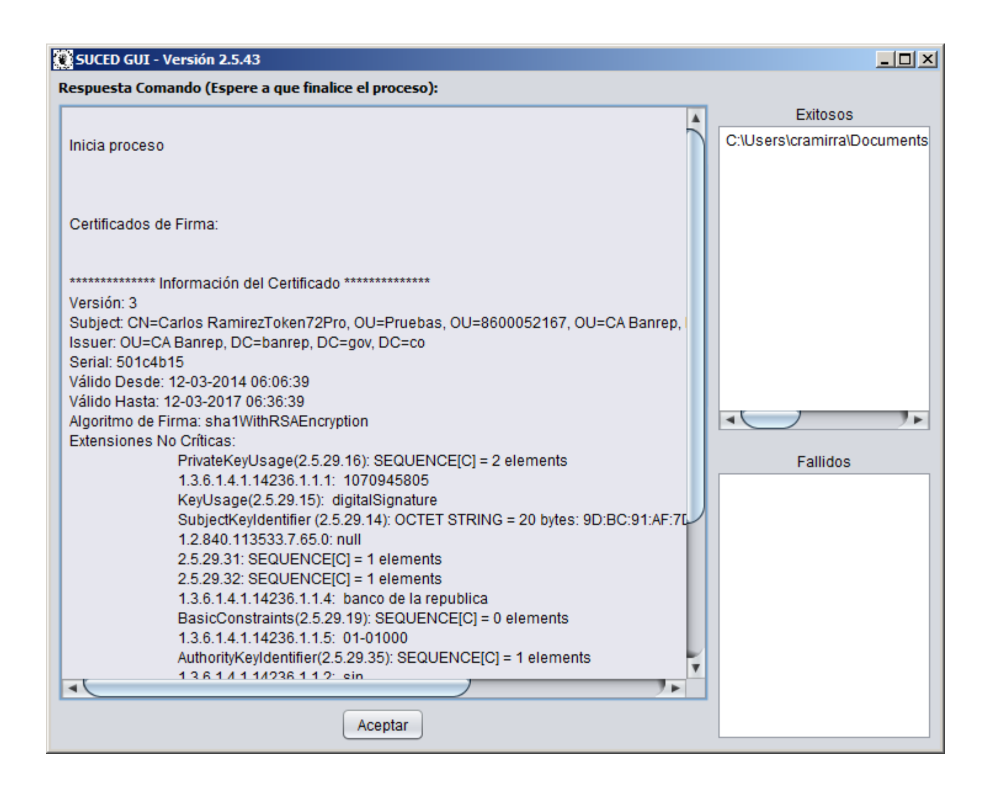
Seleccionar ***Aceptar***.

Es posible que para continuar, el sistema solicite la contraseña del Token:

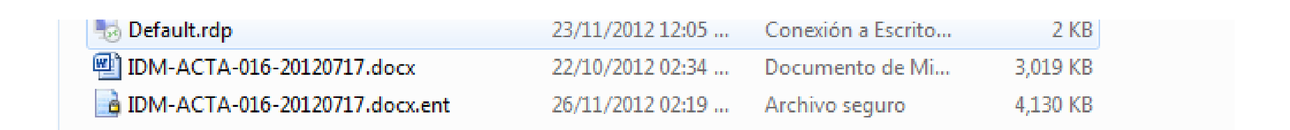




Introducir el Password del Dispositivo y hacer clic en ***Ok.***



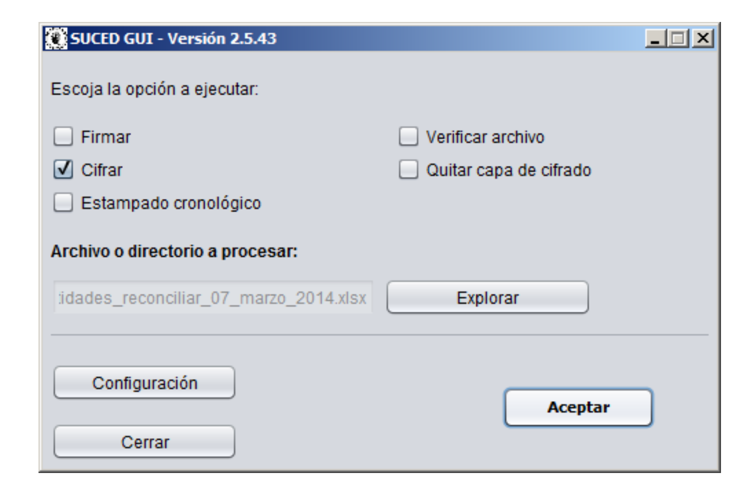
El sistema realizará el proceso de firma del archivo, y ubicara el resultante en la misma dirección del archivo de origen:



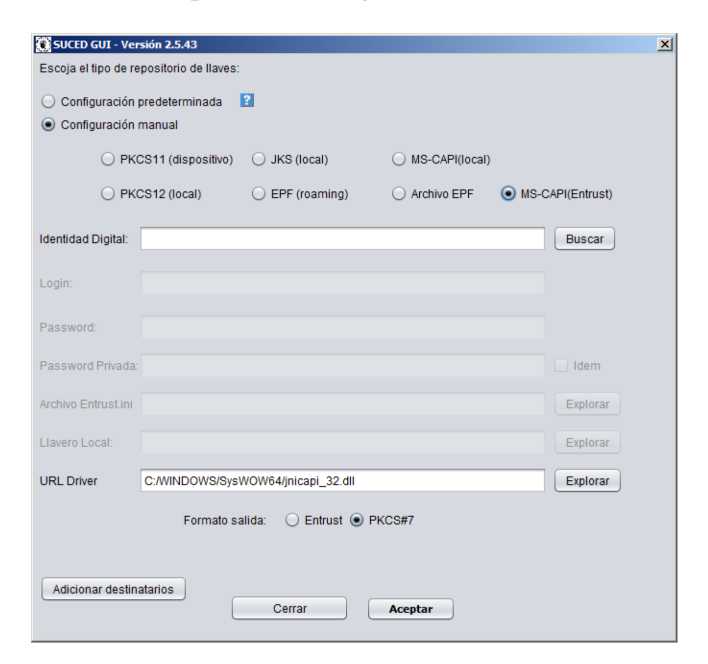


4.2 Operaciones de Cifrado

Seleccionamos la opción de cifrar:

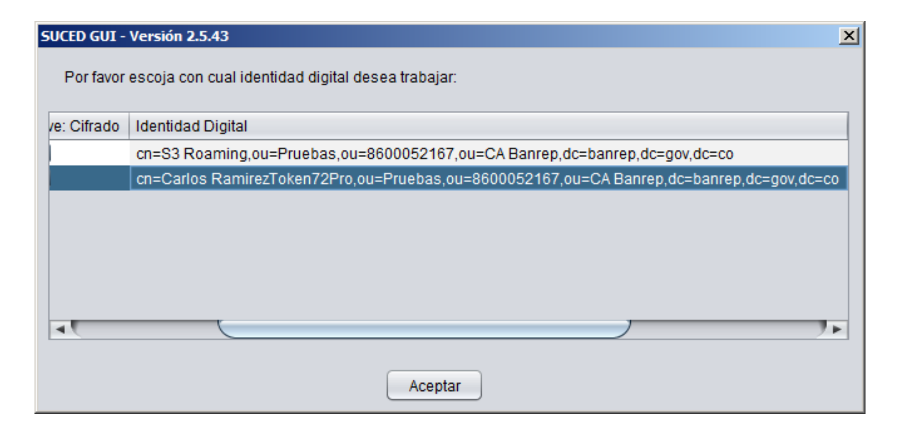


Si **NO** se han seguido los pasos mencionados en la sección "4.7 Optimización de pasos SUCED GUI", debemos elegir configuración manual y posteriormente MS-CAPI (Entrust), de lo contrario podemos usar la opción "Configuración Predeterminada":

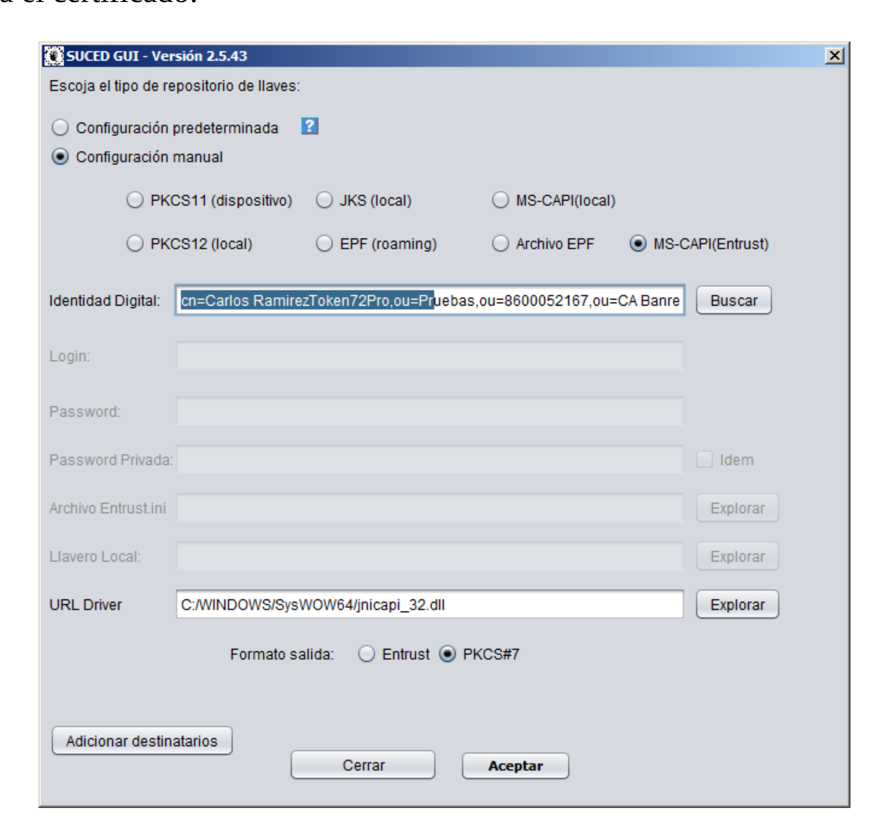




Se debe hacer clic en el botón "Buscar", se presentarán los certificados que estén disponibles para ejecutar la operación (antes debe haberse conectado el Token):



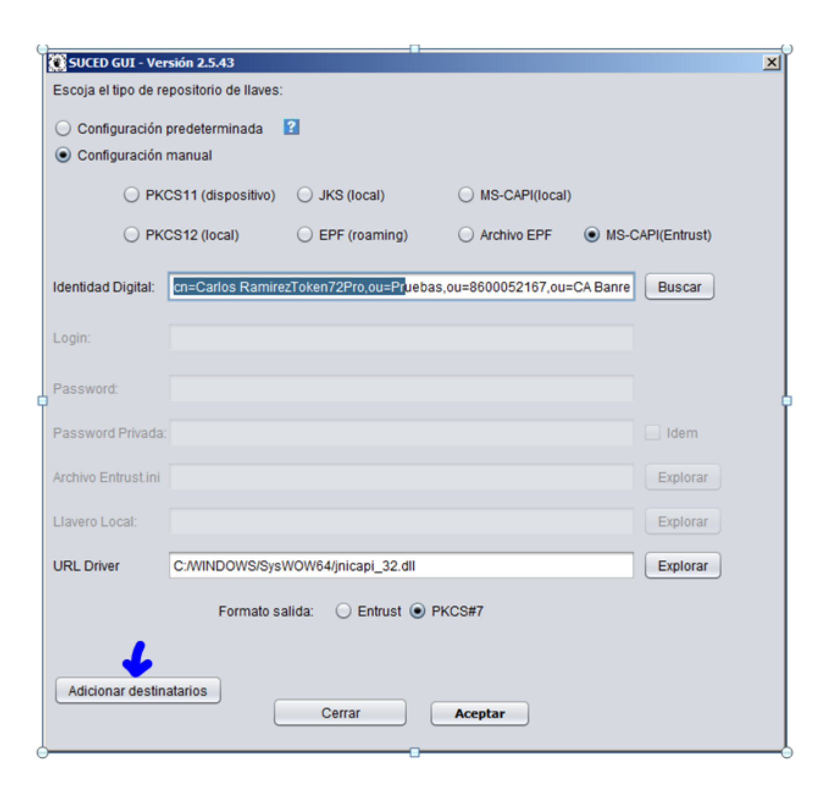
Se selecciona el certificado a usar y se hace clic en el botón "Aceptar", el sistema seleccionara el certificado:





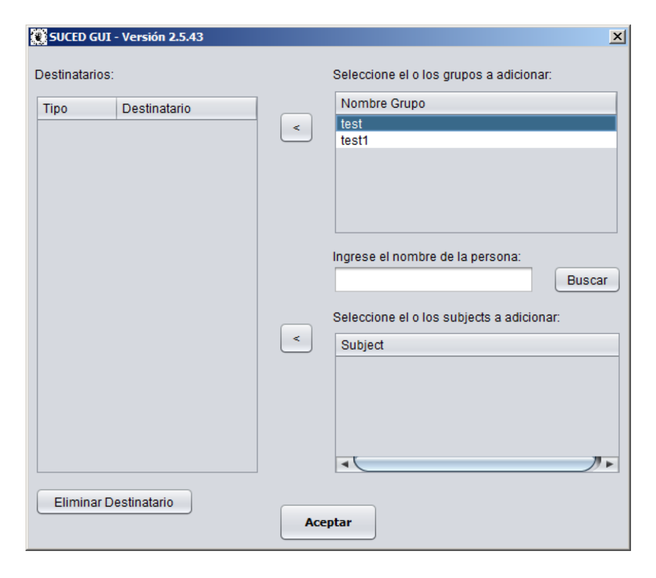
De acuerdo al formato de salida que se desee seleccionamos el formato de salida “Entrust” para generar formato .ent o “PKCS#7” para generar formato .enc.

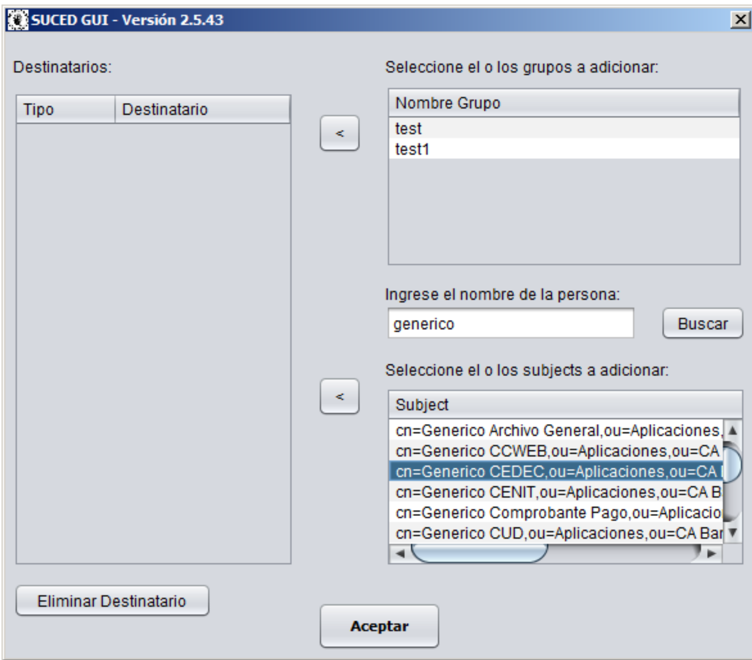
En este punto se pueden seleccionar los destinatarios favoritos previamente creados (el procedimiento de creación de favoritos se explicará más adelante), ingresando al botón respectivo llamado “Adicionar destinatarios” tal como podemos ver:





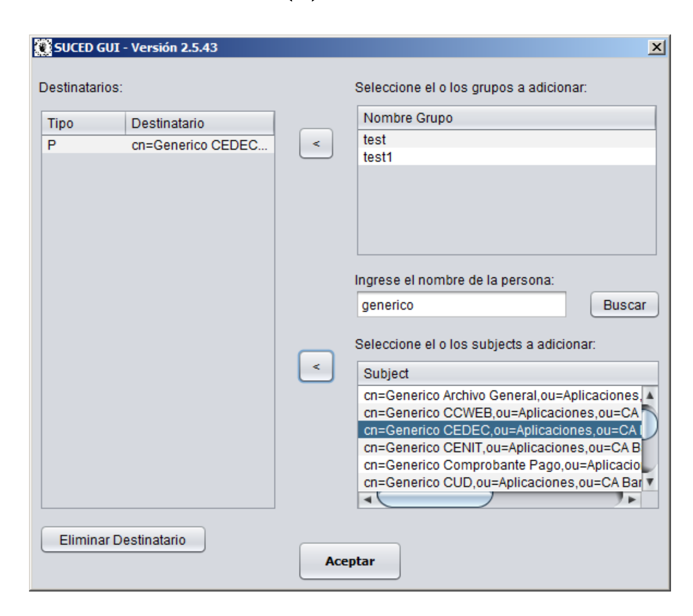
Y en campo llamado "Ingrese nombre de la persona" escribimos las primeras letras del nombre y va a presentarse el listado correspondiente tal como podemos ver a continuación:



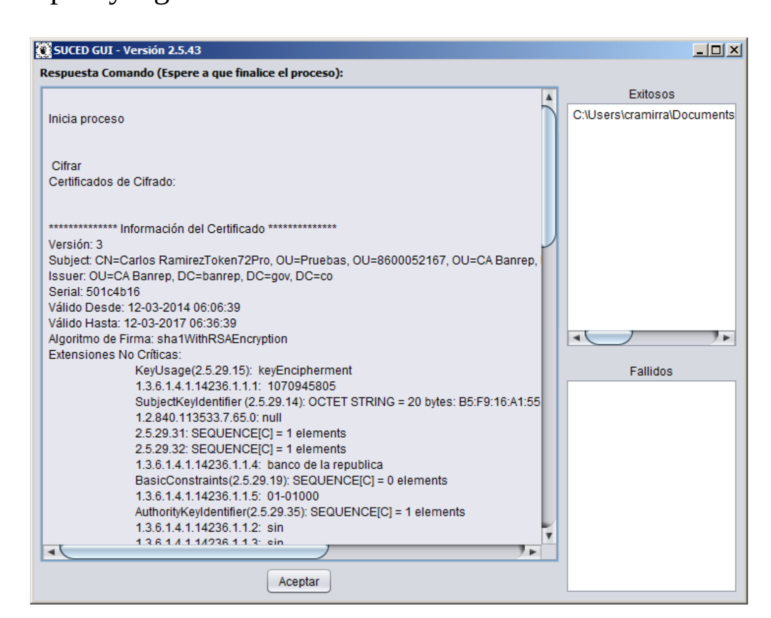




Con las flechas respectivas adicionamos los destinatarios (hacia el panel izquierdo) tanto grupos (G) como individuos adicionales (P):

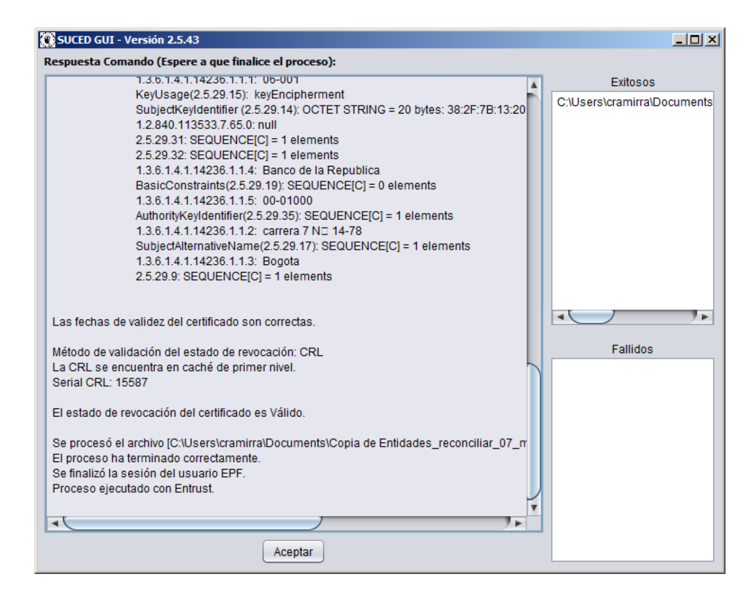


Seleccionamos aceptar y siguiente el sistema valida la información del certificado:





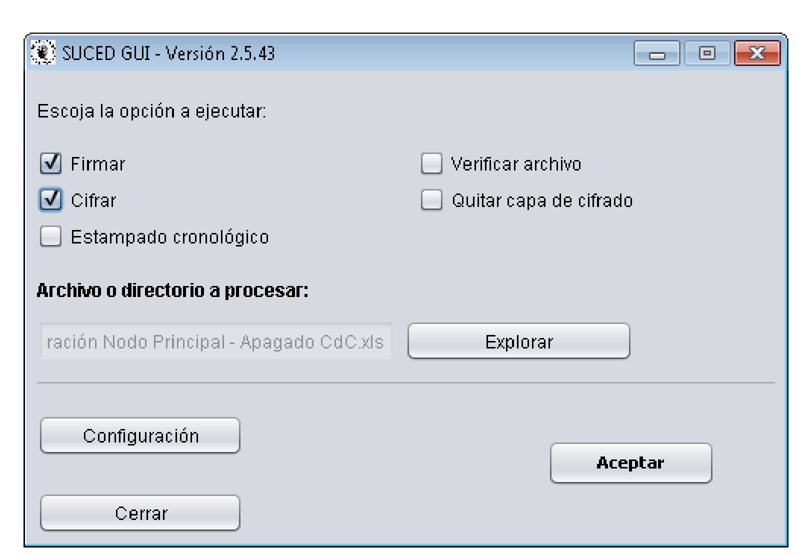
Al final del log, va a aparecer si el archivo quedó cifrado correctamente:



En donde el archivo generado queda en el mismo directorio del archivo original y seleccionamos aceptar.

4.3 OPERACIONES DE FIRMA Y CIFRADO

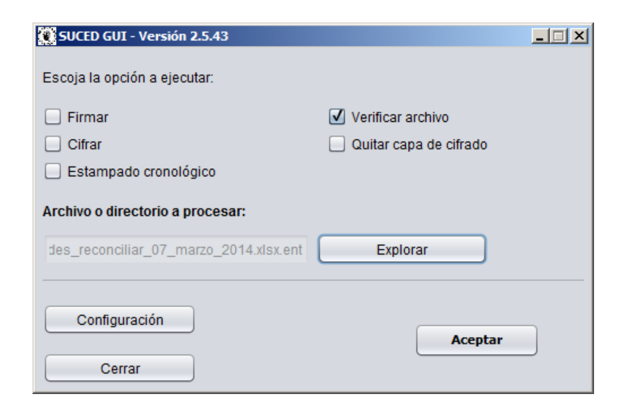
Para los procesos de firma y cifrado de archivos, se deben seguir los pasos descritos en los numerales 4.2 Operaciones de Cifrado, con la salvedad que en la opción a ejecutar se debe seleccionar la opción ***Firmar*** y la opción ***Cifrar*** al mismo tiempo.



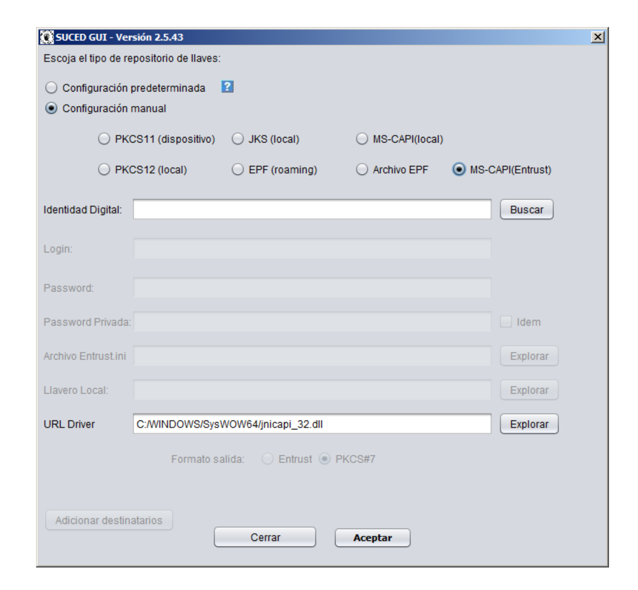


4.4 Operaciones de Verificación y descifrado

Dentro de la ventana principal de Suced, seleccionamos el botón de verificar archivo y seleccionamos el archivo para verificar en el botón explorar:

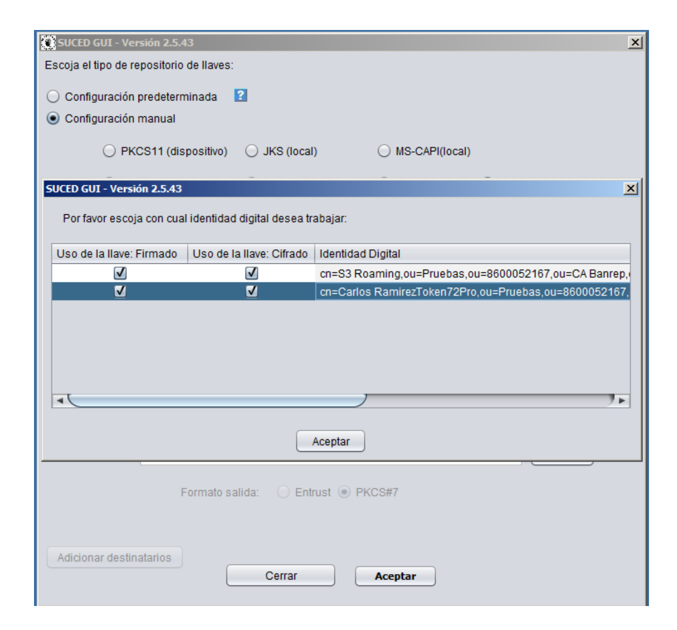


Si **NO** se han seguido los pasos mencionados en la sección "4.7 Optimización de pasos SUCED GUI", seleccionamos Configuración manual y la opción "MS-CAPI(Entrust), de lo contrario usamos la configuración Predeterminada:

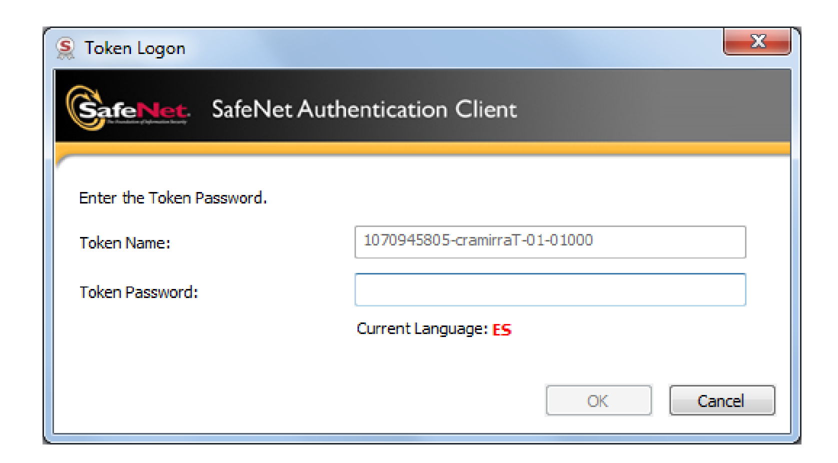




Hacemos click en el botón “Buscar”, el sistema desplegará los certificados disponibles de los cuales debemos seleccionar uno y hacer click en el botón “Buscar”: Al hacer esto, el sistema seleccionará el certificado, damos clic en el botón “Aceptar”:

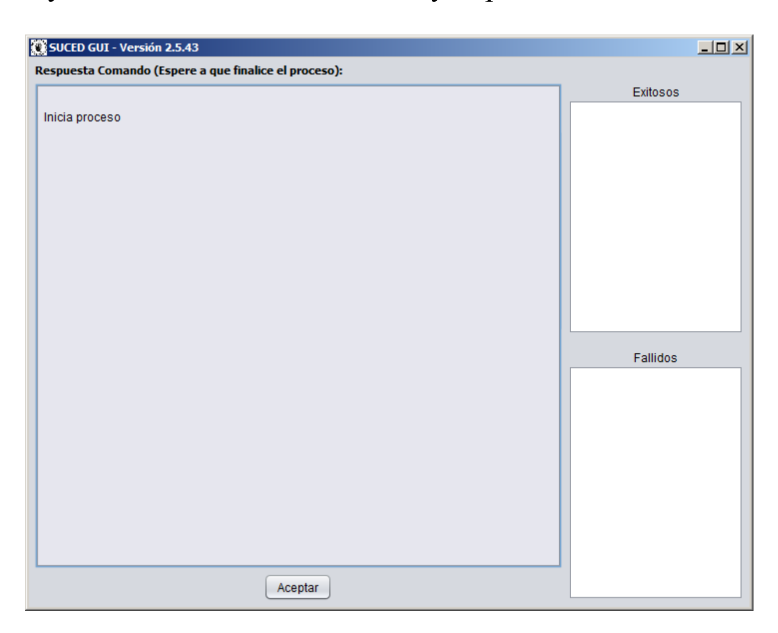


Es posible que a este punto se solicite la clave del dispositivo:

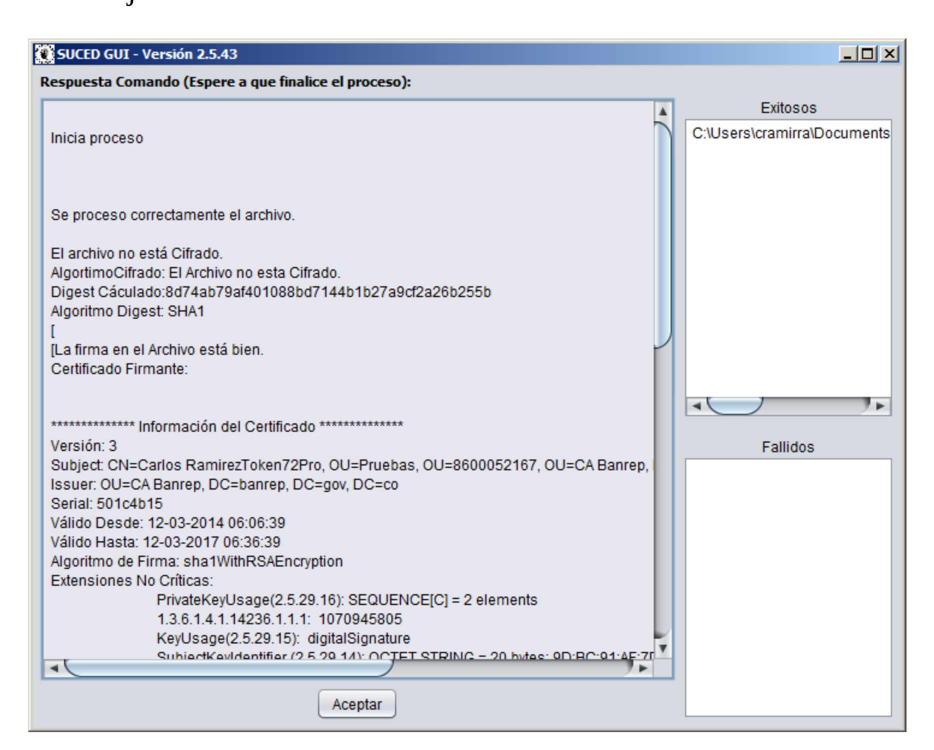




Se ingresa la clave y se da clic en el botón "OK" y el proceso iniciará:



Y aparece el mensaje de confirmación:

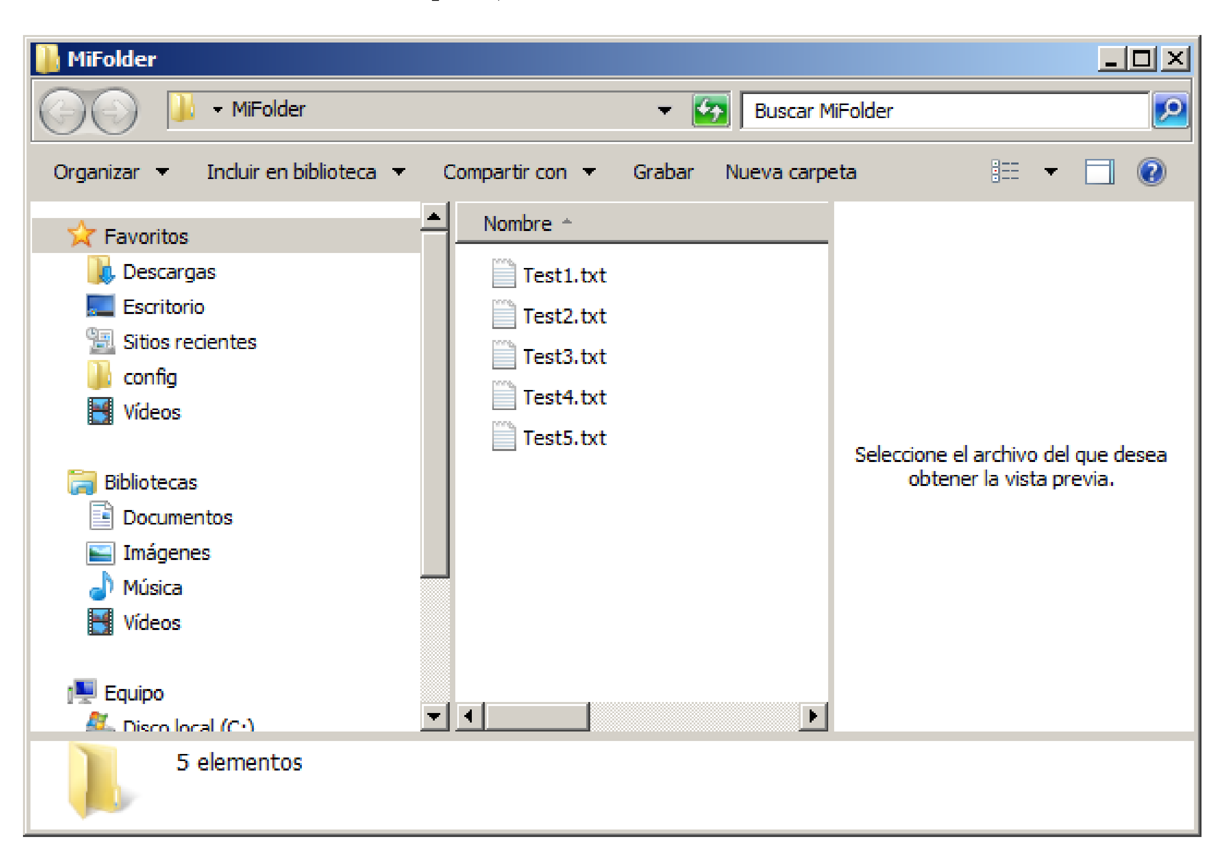




4.5 PROCESOS CRIPTOGRÁFICOS SOBRE CARPETAS

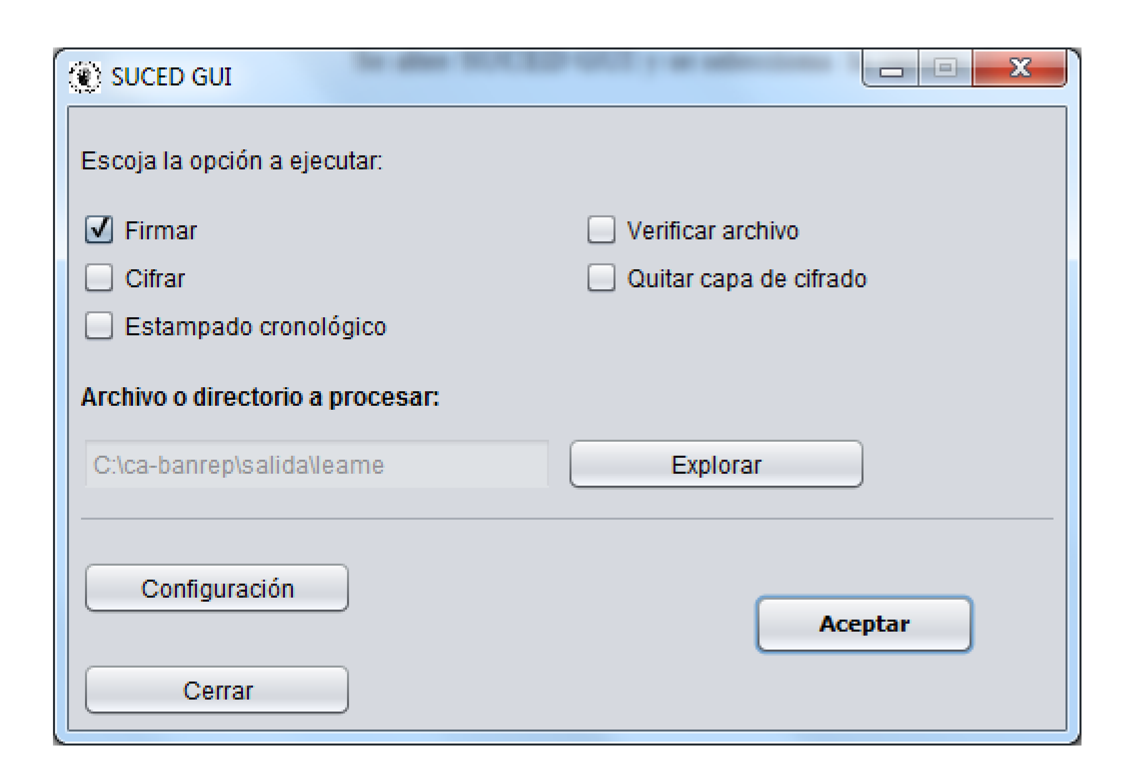
En esta sección se describen los pasos necesarios para firmar y/o cifrar varios archivos dentro de una misma ejecución, dado que generalmente tenemos que firmar y cifrar grandes cantidades de archivos, la única opción es crear una carpeta y ubicar los archivos deseados en la misma.

Se debe ubicar en una carpeta todos los archivos sobre los que se desea operar (no se hará el proceso recursivamente sobre subcarpetas):

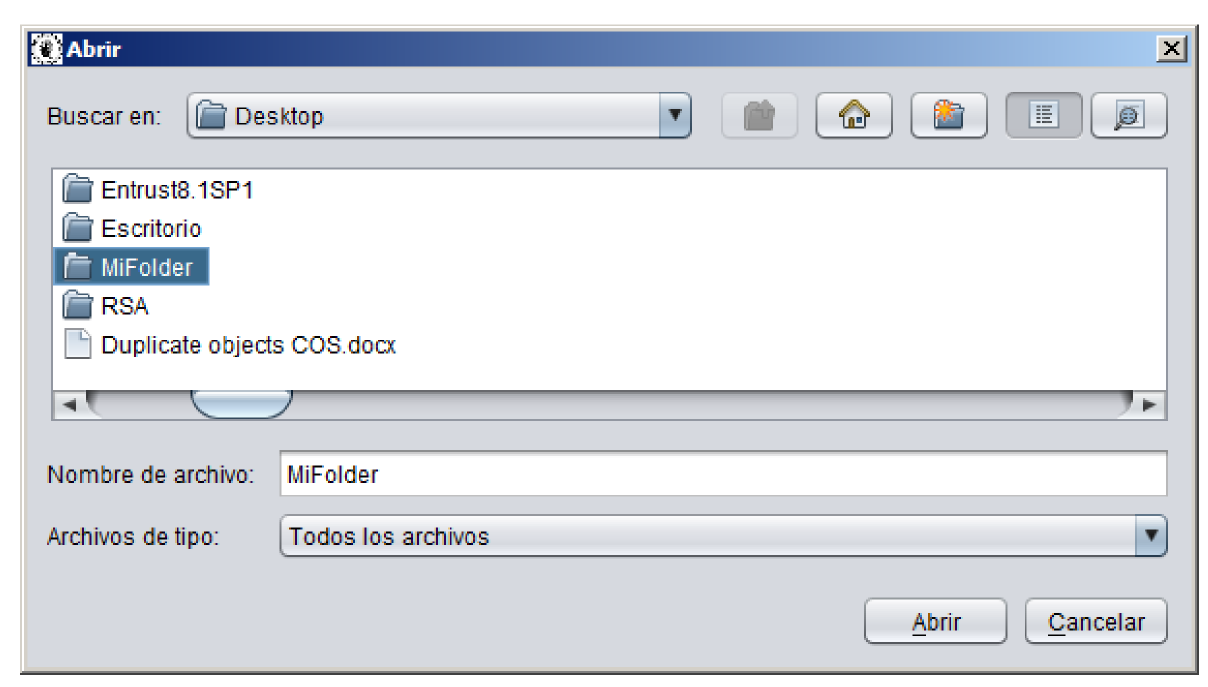




Se abre SUCED GUI y se selecciona la opción a ejecutar, para el ejemplo será "Firmar".

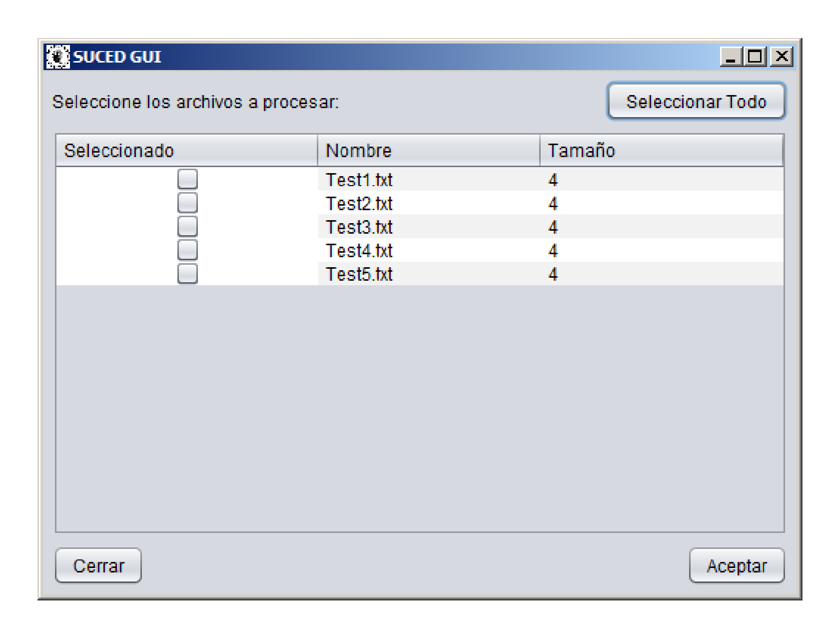


Al dar clic sobre el botón "Explorar" se selecciona el folder:

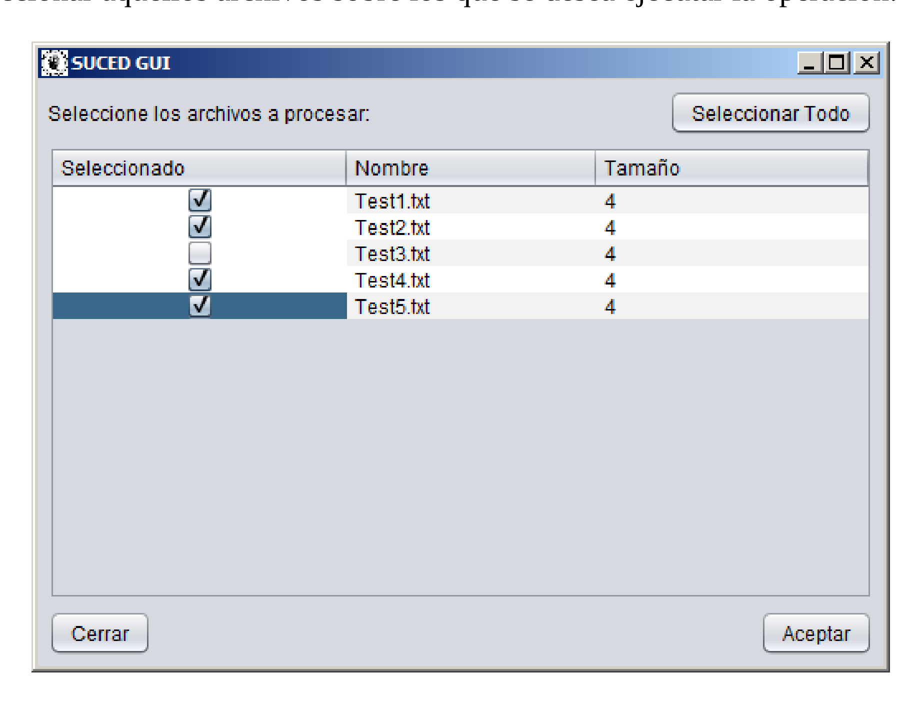




El sistema mostrará todos los archivos que se encuentren en la carpeta seleccionada:



Se deben seleccionar aquellos archivos sobre los que se desea ejecutar la operación:





Se hace clic en el botón "Aceptar" y el sistema mostrará los seleccionados, se sigue el proceso normal de acuerdo al proceso a ejecutar y a la versión del Token (el detalle en las secciones **¡Error! No se encuentra el origen de la referencia.¡Error! No se encuentra el origen de la referencia.¡Error! No se encuentra el origen de la referencia.**) y se obtendrá la finalización del proceso:

```
Respuesta comando
Respuesta Comando (Espere a que finalice el proceso):
                    1.2.840.113533.7.65.0: null
                    2.5.29.31: SEQUENCE[C] = 1 elements
                    2.5.29.32: SEQUENCE[C] = 1 elements
                    1.3.6.1.4.1.14236.1.1.4:  Banco de la Republica
                    BasicConstraints(2.5.29.19): SEQUENCE[C] = 0 elements
                    1.3.6.1.4.1.14236.1.1.5:  00-01000
                    AuthorityKeyIdentifier(2.5.29.35): SEQUENCE[C] = 1 elements
                    1.3.6.1.4.1.14236.1.1.2:  Carrera 7 N? 14-78
                    SubjectAlternativeName(2.5.29.17): SEQUENCE[C] = 1 elements
                    1.3.6.1.4.1.14236.1.1.3:  Bogota
                    2.5.29.9: SEQUENCE[C] = 1 elements



Método de validación del estado de revocación: CRL

Se actualizó la CRL en caché para el Subject: CN=Generico CENIT, OU=Aplicaciones, OU=CA Banrep, OID.
Serial CRL: 15166

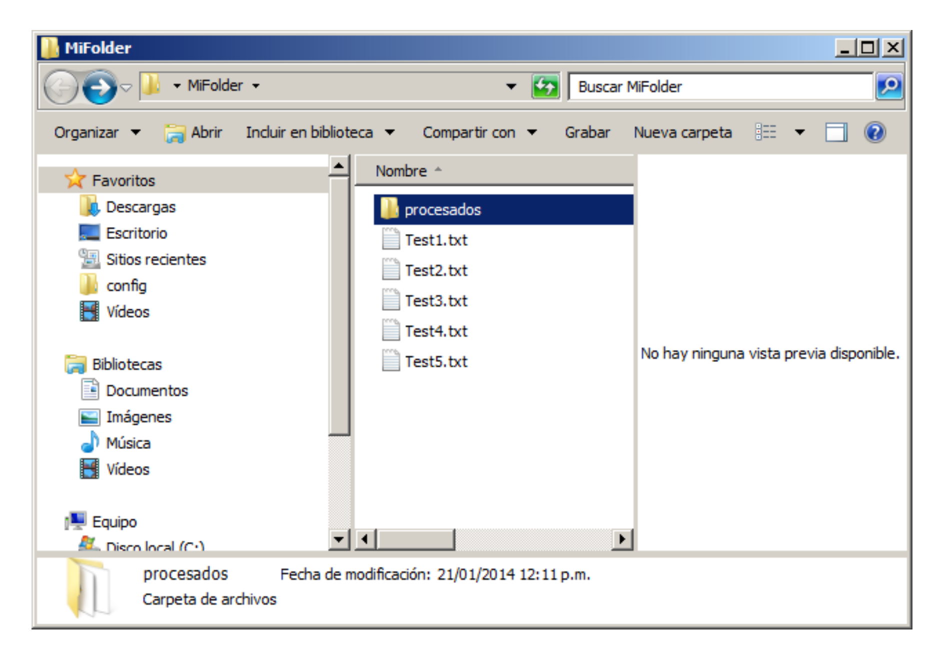
El estado de revocación del certificado es Válido.

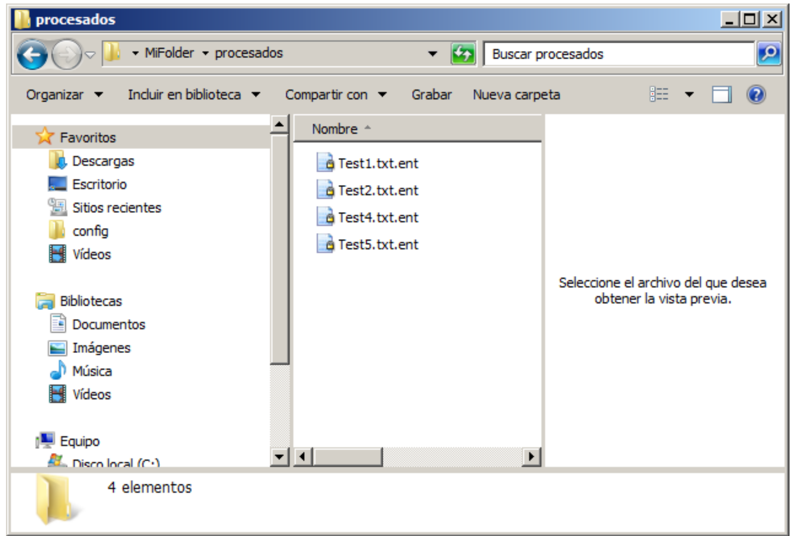
Se procesó el archivo [C:\Users\cramirra\Desktop\MiFolder\Test1.txt] criptográficamente: Firmado Cifrado
El proceso  Cifrar  Firmar ha terminado correctamente.
Se finalizó la sesión del usuario EPF.
Proceso ejecutado con Entrust.

Aceptar
```

En la carpeta seleccionada se creará una carpeta "Procesados" bajo la cual se podrán encontrar los archivos procesados.





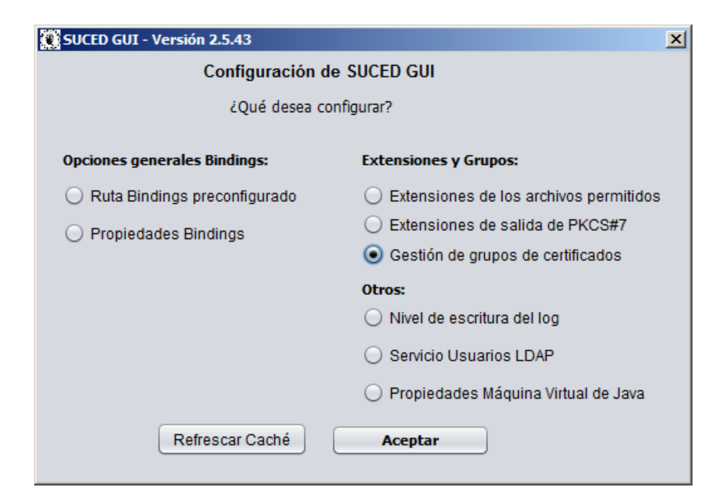


4.6 Creación de Grupos de destinatarios de cifrado

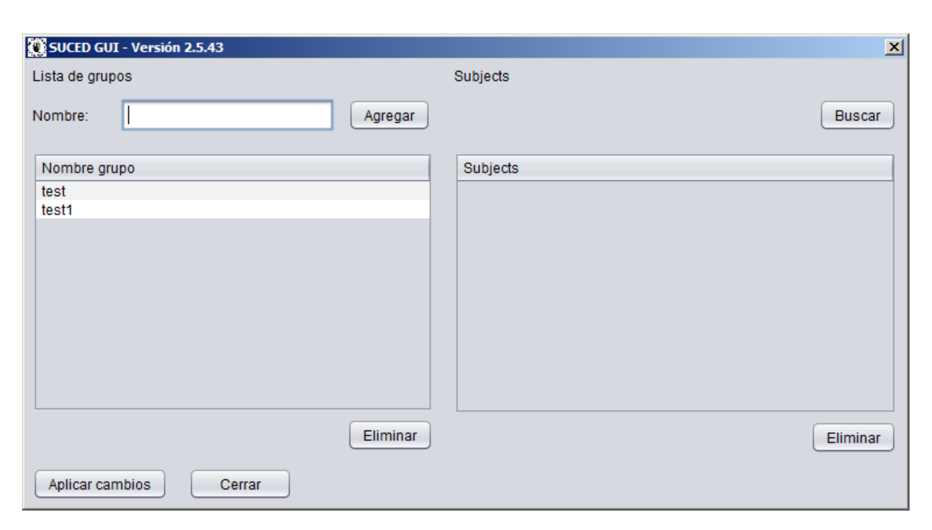
En algunos casos necesitamos cifrar archivos a las mismas personas o destinatarios, así que podemos automatizar la creación de grupos de cifrado.



Para crear grupos de destinatarios, entramos desde la ventana principal de Suced, a la pestaña “configuración” y seleccionamos el botón “Gestión de grupos de certificados” tal como podemos ver:

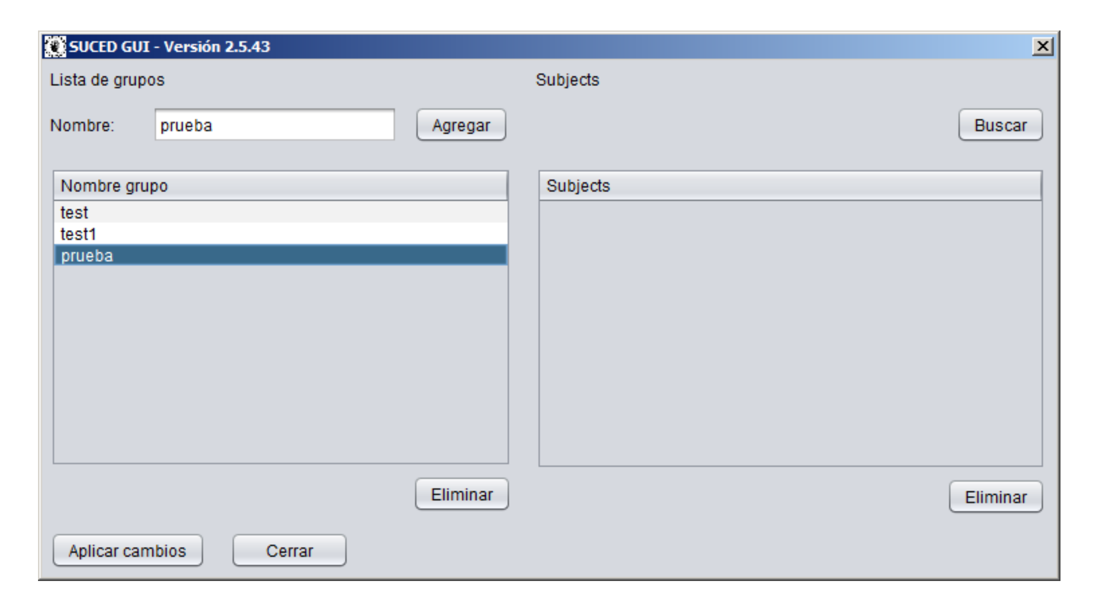


Y seleccionamos aceptar donde abre la ventana:

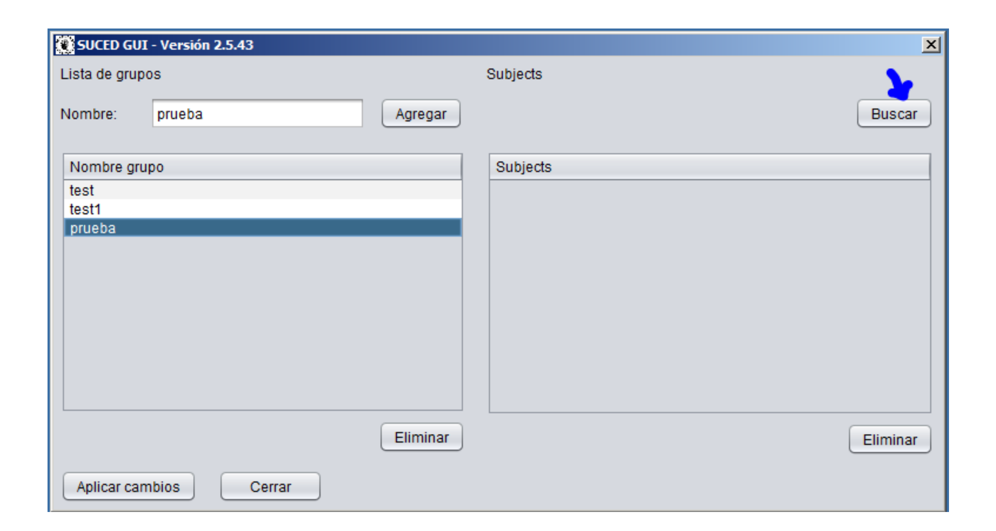


Y escribimos el nombre del nuevo grupo que deseamos crear (ejemplo: prueba)

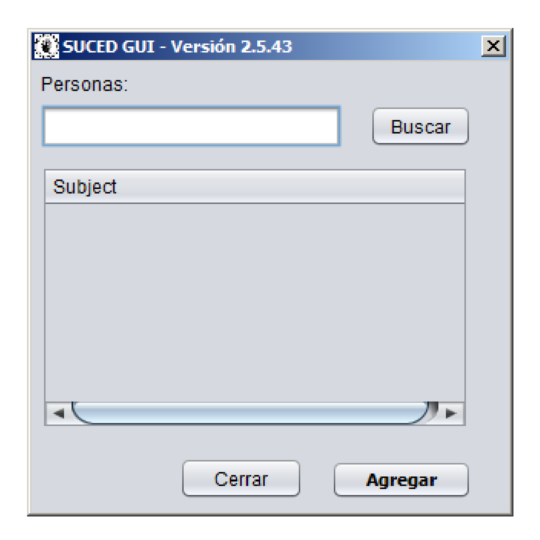




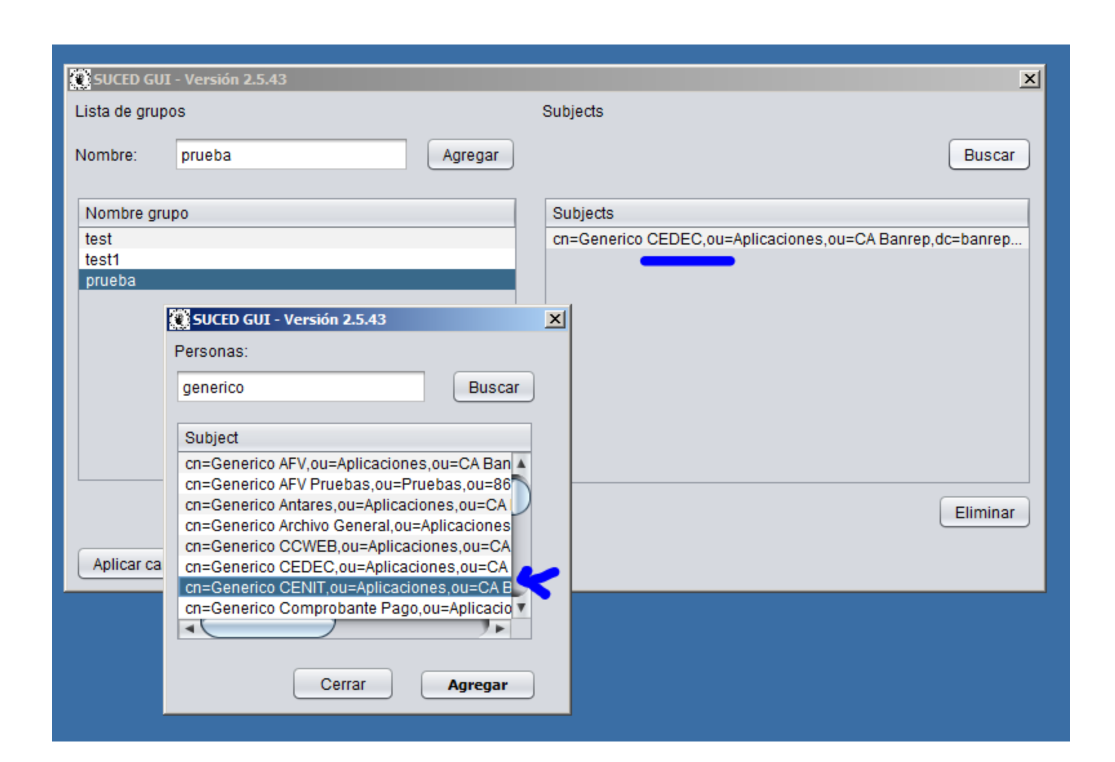
Seleccionamos agregar y luego teniendo seleccionado el grupo nuevo, vamos a la pestaña llamada "***buscar***" en donde seleccionamos los miembros para agregar a ese grupo.





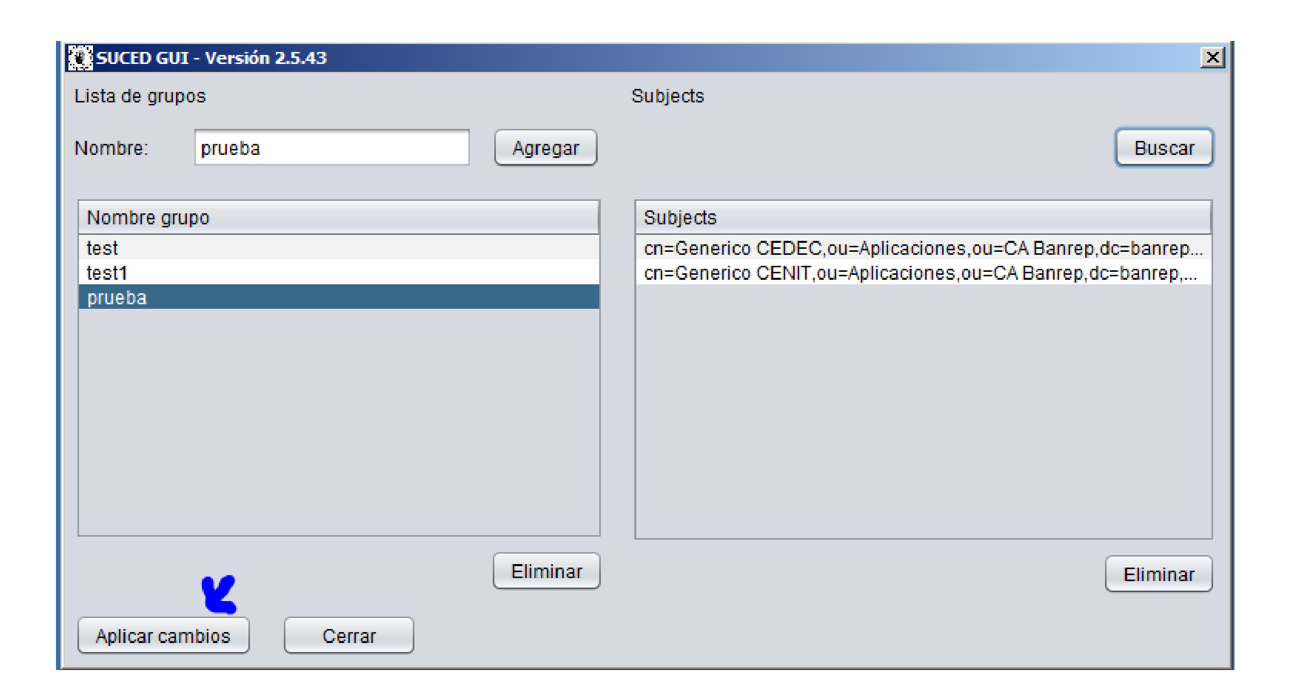


Y agregamos los usuarios respectivos.

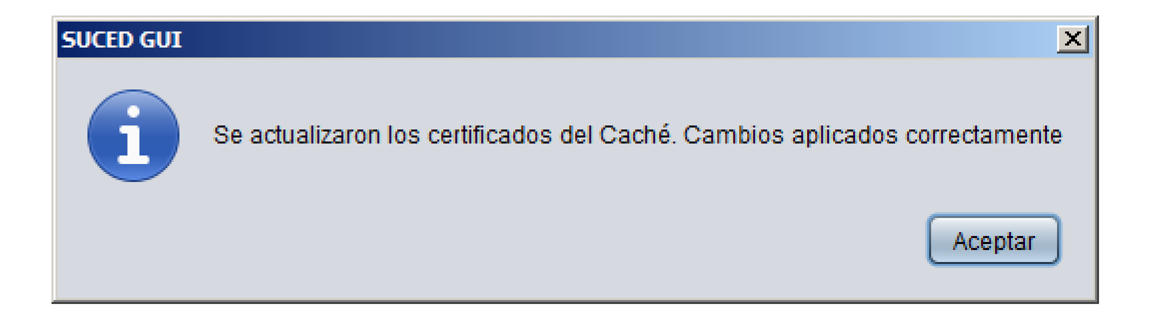




Seleccionamos cerrar, y en la siguiente ventana escogemos “Aplicar Cambios”



Si el sistema está en línea, va a salir un mensaje de confirmación como el siguiente:



Si no está en línea va a aparecer un mensaje donde no se pueden actualizar los certificados.



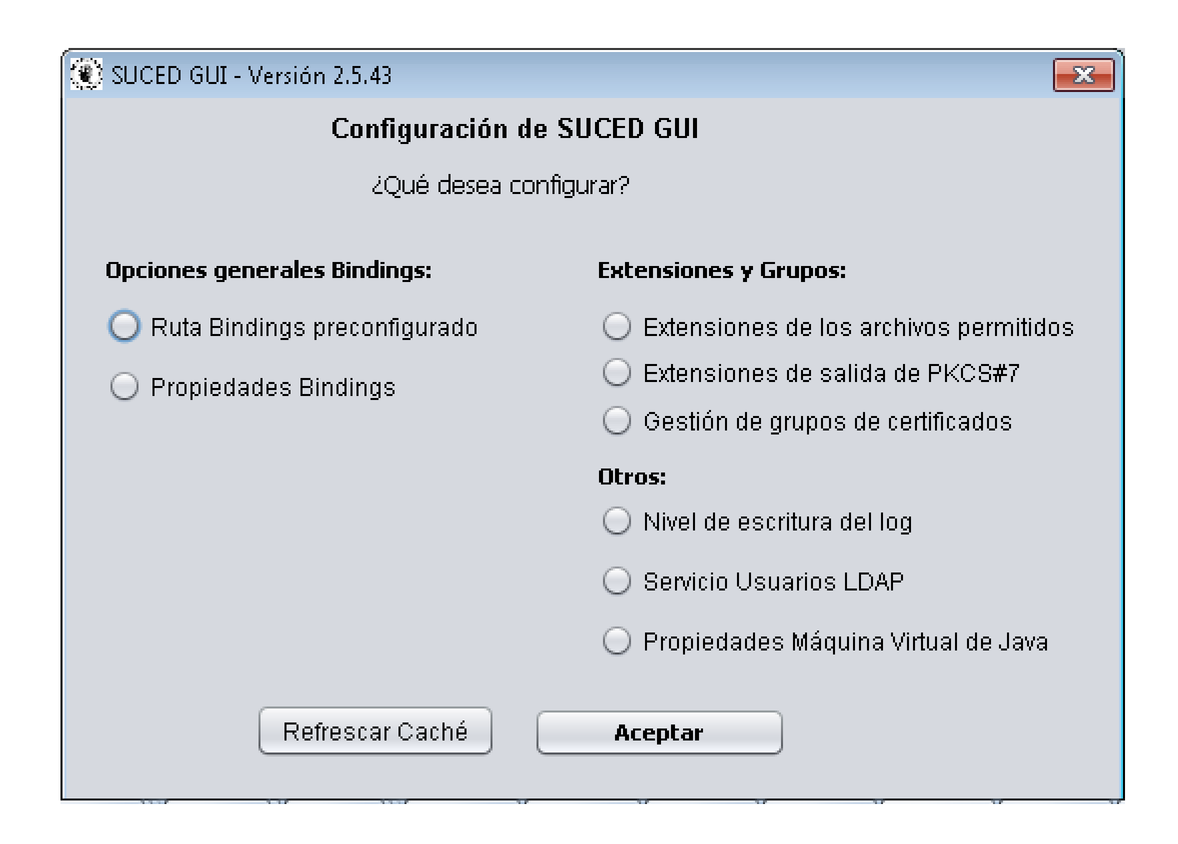
Vale la pena recordar que para actualizar los certificados de los usuarios, el sistema debe estar en línea, es decir con WSEBRA abierto y conectado.

4.7 OPTIMIZACIÓN DE PASOS SUCED-GUI

Si realizamos operaciones criptográficas en muchas ocasiones, podemos optimizar los pasos para realizar operaciones criptográficas siguiendo el siguiente consejo (solo se ejecuta una vez):

Conectemos el dispositivo Token donde se almacena el certificado.

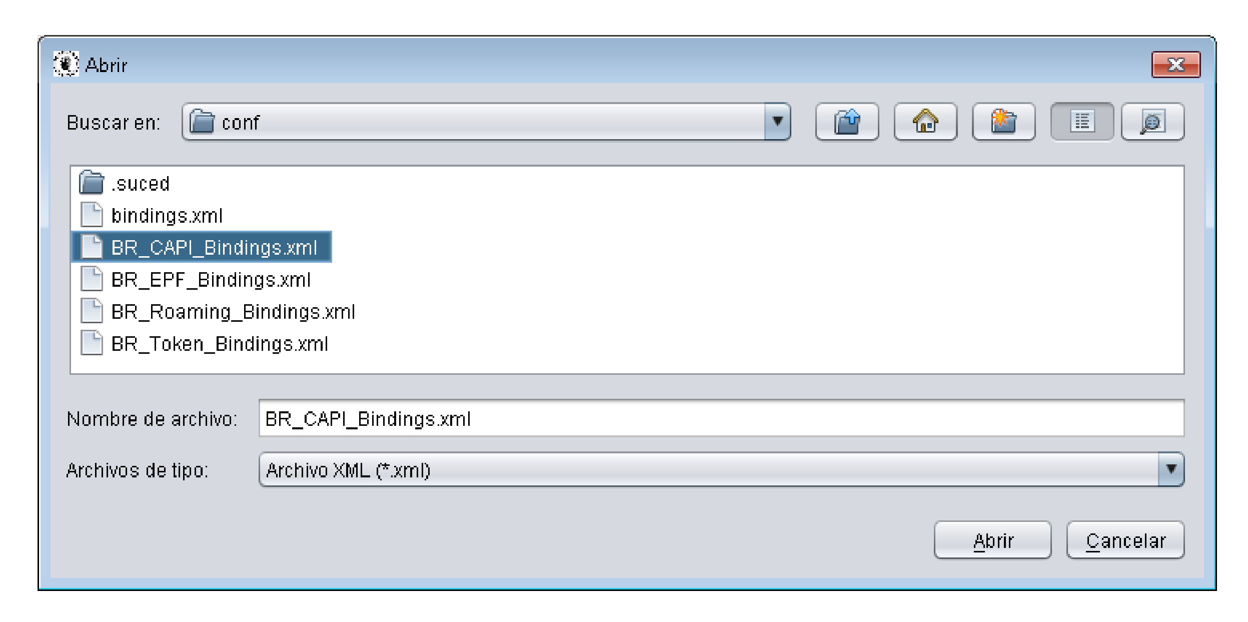
Abrir Suced-GUI y hacer clic en la opción “Configuración”:

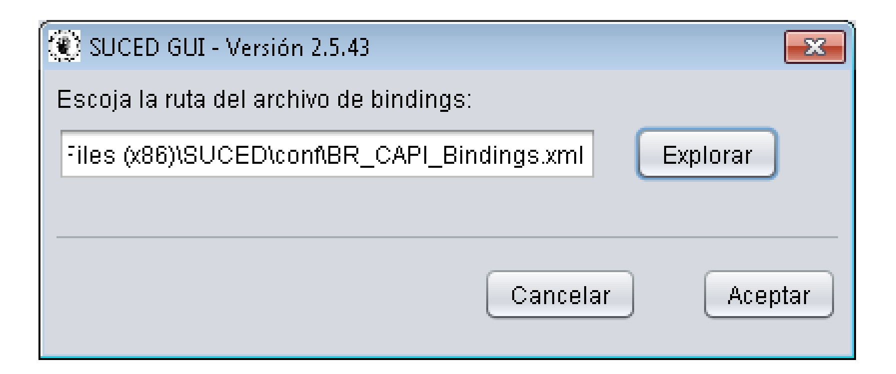




Seleccionamos la opción "Ruta Bindings Preconfigurado" y damos clic en Aceptar:

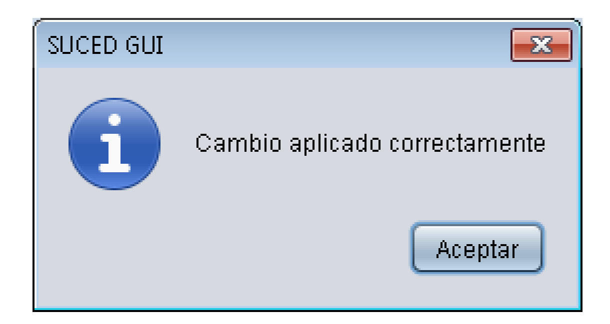
Seguidamente seleccionamos la opción Explorar y seleccionamos el Archivos BR_CAPI_Bindings.xml ubicado en la carpeta "conf" de la ruta de instalación de SUCED-GUI.



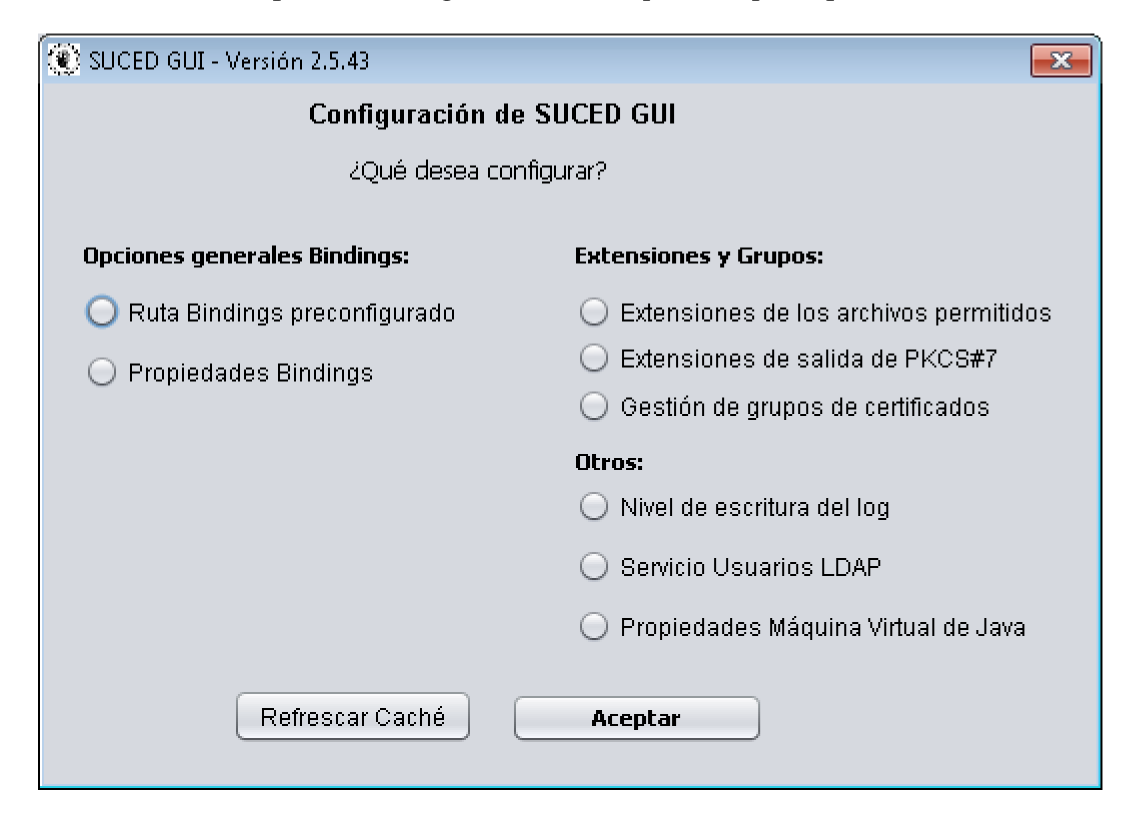


Damos "Aceptar".





Vamos de nuevo a la opción "Configuracion" en la pantalla principal del cliente SUCED:



Seleccionamos la opción "Propiedades Bindings"

Alli selecionamos la opcion "Buscar"



SUCED GUI - Versión 2.5.43

Ruta Bindings: C:\Program Files (x86)\SUCED\conf\BR_CAPI_Bindings.xml

Tipo repositorio: MS-CAPI(Entrust)

Identidad Digital: uebas,ou=8600052167,ou=CA Banrep,dc=banrep,dc=gov,dc=co   Buscar

TSA por defecto: http://ts-pki:7001/verificationserver/rfc3161timestamp

Subject TSA: CN=Timestamp Server, OU=CA Banrep, DC=banrep, DC=gov, DC=co

Ruta llavero: Explorar

Cálculo Digest: SHA1

Algoritmo firma: SHA1

Algoritmo cifrado: aes256_CBC

URL TSA: :ConsultaAutoridadTimestamp/Services/WSConsultaAutoridadTimestamp?wsdl

URL CRL: http://osb-pruebas:8011/WSConsultaCRL/Services/WSConsultaCRL?wsdl

URL Ldap: ldap://ldap-pki:1389/{0}?userCertificate;binary

URL PKI: :bas:8011/WSConsultaCertificadoPKI/Services/WSConsultaCertificadoPKI?wsdl

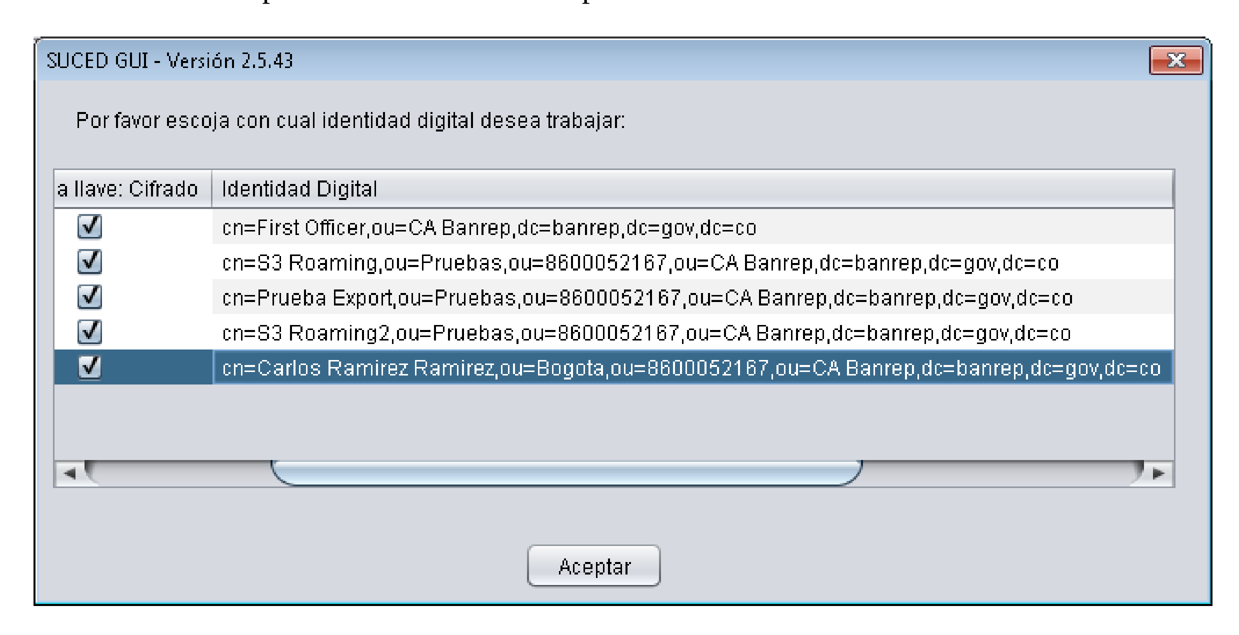
Ruta Entrust.ini: Explorar

Ruta Driver: C:/WINDOWS/SysWOW64/jnicapi_32.dll   Explorar

Cancelar   **Aceptar**



Una vez seleccionada la opción buscar, se abrirá una ventana, en donde escogeremos el certificado a usar por defecto en nuestras operaciones.



Seleccionamos "Aceptar"



SUCED GUI - Versión 2.5.43

Ruta Bindings: C:\Program Files (x86)\SUCED\conf\BR_CAPI_Bindings.xml

Tipo repositorio: MS-CAPI(Entrust)

Identidad Digital: cn=S3 Roaming2,ou=Pruebas,ou=8600052167,ou=CA Banrep,d Buscar

TSA por defecto: http://ts-pki:7001/verificationserver/rfc3161timestamp

Subject TSA: CN=Timestamp Server, OU=CA Banrep, DC=banrep, DC=gov, DC=co

Ruta llavero: Explorar

Cálculo Digest: SHA1

Algoritmo firma: SHA1

Algoritmo cifrado: aes256_CBC

URL TSA: :ConsultaAutoridadTimestamp/Services/WSConsultaAutoridadTimestamp?wsdl

URL CRL: http://osb-pruebas:8011/WSConsultaCRL/Services/WSConsultaCRL?wsdl

URL Ldap: ldap://ldap-pki:1389/{0}?userCertificate;binary

URL PKI: :bas:8011/WSConsultaCertificadoPKI/Services/WSConsultaCertificadoPKI?wsdl

Ruta Entrust.ini: Explorar

Ruta Driver: C:/WINDOWS/SysWOW64/jnicapi_32.dll Explorar

Cancelar **Aceptar**

Seleccionamos “Aceptar”.



5 GTA - MANUAL DE USO.

Consultar manual : " GTA - Manual de usuario interactivo".

6 COSTOS

Resumen de los costos asociados a SUCED:

Al Banco:

- Licencia ESP por máquina: COP 119.033,18 + IVA, por una única vez a perpetuidad.
- Soporte mensual: COP 2.259,84 + IVA.

Con el proveedor que le venda el token criptográfico

- Costo del Token criptográfico: COP 150.000, aproximadamente.
- Licencia SAC, por una sola vez (driver para que sea reconocido el Token en un PC: USD 10 + IVA.)

7 CONTROL DE CAMBIOS

31/07/2014 Carlos Ramirez - Elaboración Documento ***SUCED-Procedimiento para el uso de Automatización de procesos Criptográficos*** Versión 1.